Transitioning from Analog to Digital Communications: An Information Security Perspective

By Richard A. Dean
Department of Defense,
Fort Meade, Md 20755

ABSTRACT

This is an age of revolution in communications technology and systems. While this revolution might simply be described as a transition to digital communications technologies, these fragmented (post Bell System), market driven developments create a totally new environment to plan, influence and develop systems for the U.S. Government's secure voice users.

Secure communications depend on the availability of either end-to-end analog connections or end-to-end digital connections. The uncontrolled mixture of analog and digital links in the public switched network (and its extensions), as will happen in this digital transition, can inhibit end-to-end encryption. The introduction of security into digital systems such as Mobile Satellite, Digital Cellular Telephone, Integrated Services Digital Network (ISDN), Land Mobile Radio and other systems represents both a challenge to our existing infrastructure and an opportunity to capitalize on new technology.

This paper is the author's attempt to summarize the governments perspective on evolving digital communications as they affect secure voice users and approaches for operating during a transition period to an all digital world.

NEW DIGITAL COMMUNICATIONS

Virtually every component of the communications infrastructure will be influenced by digital technology. The critical systems affected by this transition are summarized below.

Integrated Services Digital Network (ISDN) represents the largest and most visible digital service on the horizon. ISDN will offer many new features for data and secure voice users on the Public Switched Network (PSN). The menu of services will allow backward compatibility with analog POTS service for data modems, facsimile, and secure voice users. In fact the flexibility of ISDN will facilitate some of the connection problems for other networks as described later.

Mobile communications which includes Cellular, Satellite, Land Mobile Radio, and portable phones represents today's fastest growing communications market [1]. The growth of this market and the pressure for bandwidth conservation has led to the introduction of low rate compressed voice in the range of 4-13 kbps. Because these low rate digital voice links will not support a conventional modem, and the networks do not carry the digital signal to the far end, this voice compression will challenge our ability to secure

these links. Mobile communications also represents a potential threat to sensitive U.S. communications as these radio communications will be readily available in the clear. Backward compatibility to the government's STU-III secure telephone and other secure systems will likewise be a challenge. Several systems are in various stages of development including Digital Cellular telephone, Land Mobile Radio, Mobile Satellite, and INMARSAT. Each of these systems has the potential of becoming a valuable secure communications link but each will require inclusion of features to enable secure interoperability.

INTEGRATED ARCHITECTURE

The recent explosion of new digital systems has forced a more comprehensive look at at interoperability on these systems. While each system has a unique protocol set, developing custom solutions for each new network is neither wise nor feasible. It is clear that the challenge is to conceive a plan that will enable transparent, communications among the dominant future digital systems. The interoperability challenge is to facilitate a smooth transition by maintaining backward compatibility with existing secure analog equipments. These existing and future systems consist of STU-III on existing analog POTS, Digital Cellular Telephone, Mobile Satellite, and ISDN (with a potential new terminal for that media). Managing the transition from a STU-III based (analog end-to-end) system to an ISDN based system with a large mobile user population represents a major challenge. One must either make all new terminals backward compatible at some expense, replace existing secure voice equipment with new equipment, or face the problem of building high volume gateways for interoperability. In this paper it was decided by the author to try to move forward to embrace new digital techniques for future compatibility rather attempt to maintain continued analog operation. While a centralized Gateway solution is presented, various decentralized solutions will be practical and desirable to implement in specific instances. A family of compatible solutions are in fact possible in concept and such a set of solutions might be necessary to resolve the anticipated bulge that will appear in the 1994-98 timeframe when we are in the midst of the transition from analog to digital. Key to the success of such an architecture, however, is to develop a common interface with mixed digital systems that will allow transparent end to end digital operation.

In looking at alternatives for a global connection architecture, there is an option to resolve the interface problem with a distributed solution or with a centralized solution. A distributed solution deals with the interface problem by a translation for compatibility at each end terminal or as close to that terminal as possible. A centralized solution performs the translation at one central location. Both approaches have advantages. The approach presented here shows an evolution from a distributed solution to a centralized solution using a Gateway.

The architecture is presented in three phases consistent with developments in the associated usage and availability of the

Cellular, Mobile and ISDN services.

The architecture for Phase 1 is shown in Figure 1. This is a distributed solution using STU-III modem pools (shown as M-3) to perform analog to digital transition for Mobile Satellite and Cellular. The STU-IIIB uses a direct (black) digital output for mobile applications. It is shown for the 1990-93 time frame where the extent and geographic distribution of this solution is limited. This approach maintains the digital nature of the mobile network and its interface is the same as most other digital users.

An architecture for Phase 2 is shown in Figure 2 for the timeframe 1994-1998. This represents the peak of the analog to digital transition where it is expected that there will be large numbers of both digital and analog secure systems connected. In this case the Gateway is the primary place where the mobile systems transition to analog STU-III terminals. This is performed by establishing a digital connection (switched or dedicated) from the Mobile and Cellular interfaces to the Gateway. The M-3 modems shown in figure 1 are relocated at the Gateway. The digital interface shown as G is a simple (assumed standard) digital interface to the Mobile and Cellular interfaces. Figure 2 also shows an early ISDN network. The early ISDN terminals are assumed to be STU-III interoperable (direct or virtual) and include a STU-III modem. This is provided so that the Gateway traffic and resulting blockage is limited. ISDN will also provide a simple and cheap switched connection from the Mobile and Cellular interfaces and the Gateway. Figure 2 also shows a STU-IIIB (a STU-III with BLACK digital output) coupled directly into ISDN with an ISDN adapter. The incorporation of this adapter allows direct digital communication of these STU-III's over ISDN with mobile STU-III's and with ISDN terminals. The use of analog modems in the ISDN terminal and the use of ISDN adapters on STU-III's provide users options to enhance their grade of service and limit traffic through the Digital Gateway.

An architecture for Phase 3 is shown in Figure 3. This is the architecture for the period 1999 and beyond. In this era ISDN is almost universally available. Mobile and Cellular operation is supported by direct end-to-end BLACK connections directly to ISDN terminals via a simple (assumed standard) digital interface. The Digital Gateway continues to operate, however, as an interface to the remnant of analog STU-III users. These may be people at remote locations or international service where end-to-end digital is unavailable. The M-3 modems are removed from the ISDN terminals and can be used at the Gateway.

The centralized solution has several inherent advantages. This solution lumps most of the interoperability problems into a single solution where it is assumed that economies of scale will reduce overall costs. Our requirements to each of the numerous communications carriers is uniform and standard. We simply want to pull out the embedded 4.8 kbps stream from their system and port it to the Gateway on a standard digital link. We eliminate the need for a custom, government owned M-3 modem pool at geographically and organizationally diverse facilities. We trade off this widely dispersed logistics problem against the

communications costs to connect to a centralized, more efficient facility. Transition to an all digital environment is clear. When direct end-to-end digital connections can be made from the mobile interface to the ISDN user, the central Gateway is bypassed. Finally, when the bulk of the users are connected to ISDN on either an ISDN terminal or a STU-III with a terminal adapter, the gateway can be used to extend service to the remnant of analog STU-III users.

MOBILE SATELLITE INTERFACE

The proposed interoperability scheme requires a common set of features be provided by mobile cellular and satellite systems. A preliminary evaluation of the systems function reduces these to the following:

1. Recognition by the host system of the STU-III capability at the mobile unit.
2. Enable the insertion of an encrypted data stream in place of the 4.8 kbps speech data within the packet structure and removal at the other end (mobile or PSN interface) with transparency.
3. Include the control signaling to allow either the mobile STU-III or the PSN STU-III to switch from clear voice to secure voice and back at will. In the case of the PSN interface, a 2100 Hz tone is the signal used to bring in the STU-III modem.(Phase 1)
4. Support a STU-III modem pool at the PSN entry.(Phase 1)
5. Include the interface and control necessary for direct transfer of the 4.8 kbps data to a remote facility by either a dedicated or switched fractional T1 link or ISDN when available.(Phase 2)
6. Perform all system signaling out of band after the call has been established.
7. Maintain synchronization and bit integrity for the 4.8 kbps stream after the connection is established.
8. Incorporate the Fed. Std. 1016 4.8 kbps CELP voice coder as the standard speech algorithm for both clear and secure.

These functional requirements are judged to be straightforward to implement if identified in the early design phase of the mobile system. These features are also similar to the requirement of many other data a facsimile users who need to interoperate on mobile systems.

CONCLUSIONS

A concept for secure voice interoperability on emerging digital systems was presented. The transition period from analog to digital systems is handled by modem pools and a central Gateway. Long term compatibility is satisfied by an end to end connection via ISDN. The interface requirements for digital systems such as Mobile Satellite were presented and are straightforward and similar in nature to the needs of other data and facsimile users.

REFERENCES

1. M. Bonatti et al., "Telecommunications Network Design and Planning", IEEE Journal on Selected Areas of Communications, Vol 7, Number 8 Oct 1989

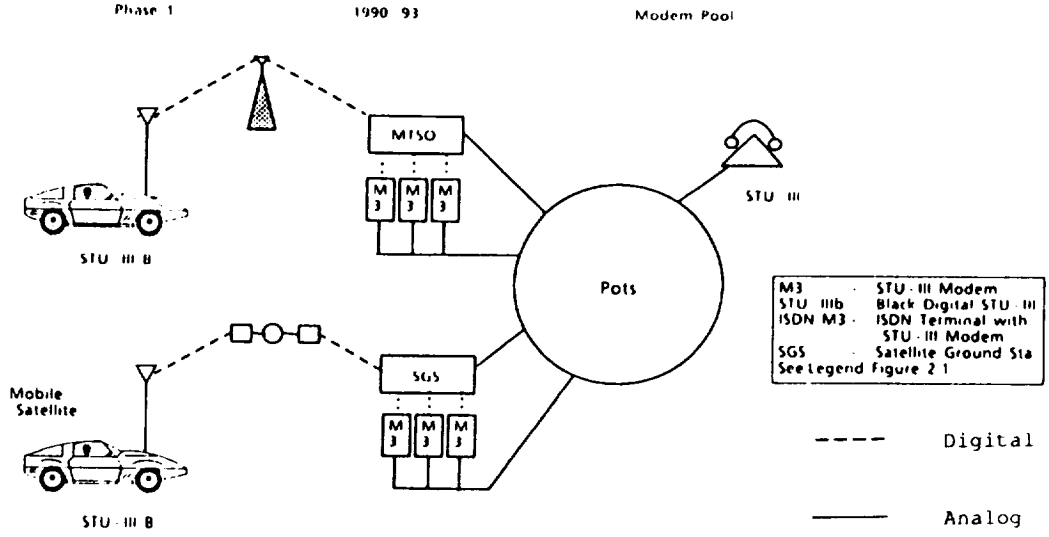

Figure 1 Phase 1, Distributed Solution with Modem Pool

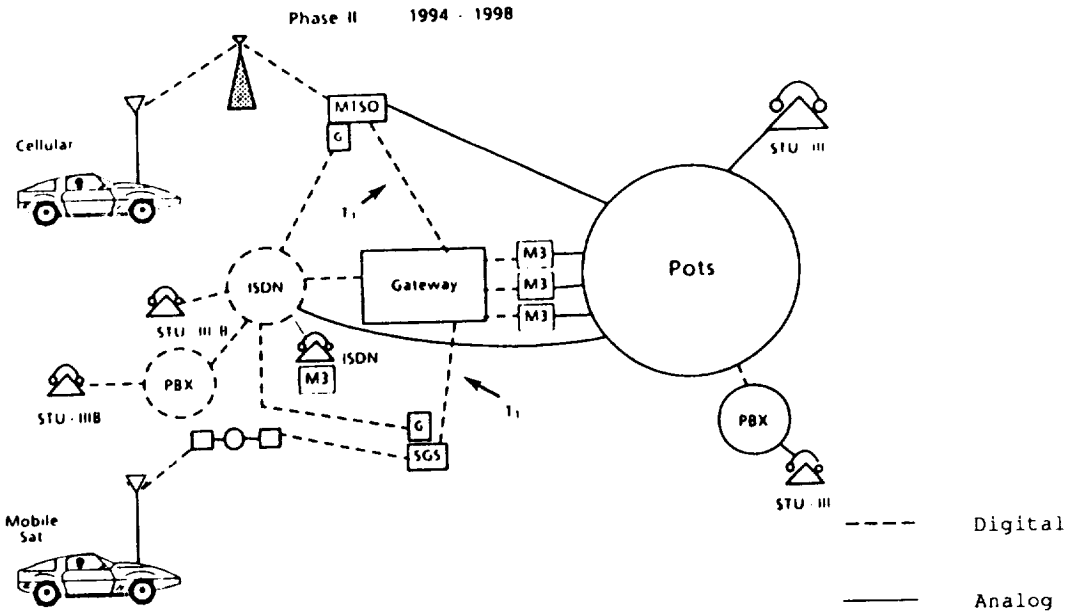

Figure 2 Phase 2, Mixed Analog/Digital Network with Gateway

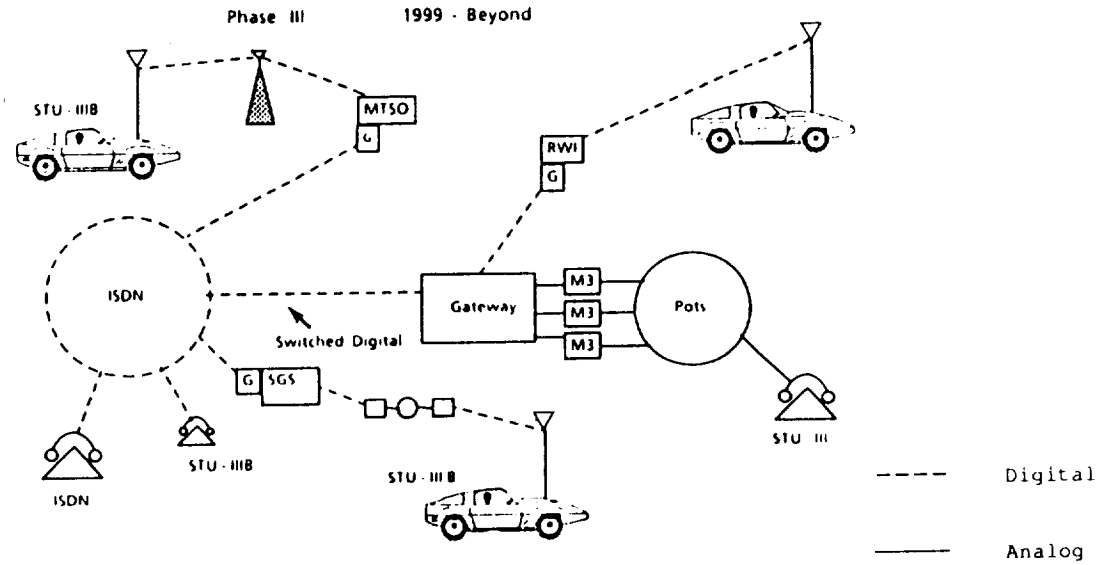

Figure 3 Phase 3, Digital Network with Analog Enclave